Unsealed MD 5/8/08 KM

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

ORDERED SEALED BY COURT

'08 MJ 1250

In the Matter of the Search of

Omniture, Inc.
San Diego Network Operation Center
Located within Level 3 Communications
8929 Aero Drive
San Diego, California

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER:

I, Travis F. Johnson, being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason to believe that on the property or premises known as:

See Attachment A-1

in the Southern District of California there is now concealed a certain person or property, namely:

See Attachment B-1

which is:

Evidence, fruits of crime, property designed for use or used in committing criminal offenses including violations of Title 18, United States Code, Sections 1030(a)(2) and 875(d). The facts to support a finding of probable cause are as follows:

See attached Affidavit of Travis F. Johnson continued on the attached sheet and made a part hereof. X Yes ______ No

TRAVIS F. JOHNSON
Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence
April 23, 2008 at San Diego, California:

HONORABLE JAN M. ADLER
UNITED STATES MAGISTRATE JUDGE

Attachment A-1

Omniture, Inc. San Diego Network Operations Center located inside the Level 3 Communications datacenter, 8929 Aero Drive, San Diego California.

ATTACHMENT B-1

The computer server owned by Bruce Mengler and using Internet Protocol Address 208.33.48.145 is subject to seizure pursuant to this warrant. The server may then be imaged and searched for evidence that Bruce Mengler accessed the computer network of Maserati North America without authority, including the website www.maseratiamerica.com, and obtained customer records and issued an extortionate threat to Maserati North America in violation of Title 18, United States Code, Sections 1030(a)(2) and 875(d). This authorization includes the search of electronic data to include deleted data, remnant data and slack space and will be conducted in accordance with paragraph 17 of the affidavit submitted in support of this warrant. Items to be seized includes the following:

a. All computer systems, software, peripherals and data storage devices.

b. All temporary and permanent files and records of any kind relating to Maserati North America including but not limited to computer logs, database files and communications;

c. All temporary and permanent files and records reflecting unauthorized access to the Maserati North America computer network; and,

d. All records and documents that identify the person(s) using any seized computers.

AFFIDAVIT

Travis F. Johnson, being duly sworn, deposes and says as follows:

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the San Diego Division. I have been employed as a Special Agent of the FBI for five years, and have been involved in investigations of computer related crimes for approximately two years. I have participated in the execution of search warrants for documents and other evidence, including computers and electronic media, in computer intrusion, intellectual property rights, and Internet related child pornography cases.

2. I make this affidavit in support of an application by the United States of America for the issuance of two search warrants: a warrant to search the residence of Bruce Charles Mengler ("Mengler"), 682 Via De La Valle, Solana Beach, California 92075, and which is more fully described in Attachment A, for the items described in Attachment B; and, a warrant to search Omniture, Inc. San Diego Network Operations Center located inside the Level 3 datacenter at 8929 Aero Drive, San Diego, California, as described in Attachment A-1 for the computer server owned by Bruce Mengler and hosted on the Omniture network at IP address 208.33.48.145 and other items as provided at Attachment B-1.

3. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of victims; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and

circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. As provided below, there is probable cause to believe that Bruce Mengler violated federal criminal laws, including Title 18, United States Code, Section 1030(a)(2) and 1030(c)(2)(B)(i) - intentionally accessing a protected computer without authority and obtaining information for private financial gain; and, Title 18, United States Code, Section 875(d) - Extortion. There also is probable cause to believe that evidence pertaining to these offenses will be found at Mr. Mengler's residence and in Mr. Mengler's personal computers as well as in the server owned by Mr. Mengler hosted at Omniture, Inc.

FACTS SUPPORTING PROBABLE CAUSE

Background

4. Maserati is a manufacturer of luxury cars headquartered in Modena, Italy. In 2002, Maserati North America (MNA) was established to import Maserati cars, manage the Maserati brand, and serve Maserati customers in the United States and Canada. One function of MNA is to conduct promotional campaigns which generate business at Maserati dealerships throughout the United States.

5. In early 2008, MNA conducted a promotional campaign by mailing flyers to potential customers. The list of customers was obtained by MNA through the purchase of lead database information from

vendors that specialize in identifying individuals having an interest and the financial means to purchase an exotic car. Customers receiving the flyer were invited to test drive Maserati GranTurismo or Quattroporte model cars in order to receive a gift certificate redeemable at Omaha Steaks.

6. To receive their gift certificate, the flyer instructed customers to visit the MNA promotional web site at www.maseratiamerica.com/omaha, login using a unique Personal Identification Number (PIN) printed on the flyer, and print a confirmation page to bring with them to a Maserati dealership during their test drive. Each customer that logged into the promotional web site using their PIN would complete a survey and review their name and contact information for update prior to printing the confirmation page. Contact information presented for review by the customer included their name and address to which the flyer was sent. Additional information collected from the customer after login included their email address and telephone numbers. Once the customer completed the survey and updated their contact information, they would submit the information to update MNA's database and print a confirmation page that would be surrendered to a Maserati dealership at the time of their test drive.

7. Each customer PIN contains 10 alphanumeric characters and is comprised of a two letter date code, followed by a two letter dealership code, and a six digit random number. An example PIN would be ECSD123456, where "EC" represents the date the flyer was mailed, "SD" is the code of the dealership located closest to the customer,

and "123456" is a unique random number associated with the customer record.

8. MNA web servers hosting the maseratiamerica.com domain are located at the company headquarters in Englewood Cliffs, New Jersey.

Notification of Security Breach

9. On March 11, 2008, an email was sent from sol.beach@gmail.com to several MNA employees and one CNH employee. CNH provides financing for Maserati cars in the United States. The email advised that their customer data had been mined from the MNA promotional web site and that this information would be publically disclosed if MNA did not "buy" silence from the sender. Provided below is an excerpt from body of the message:

> *Folks,*
>
> *You sent out a mailer enticing folks with free Omaha Steaks in exchange for a test driver.*
>
> *What you got is a potential PR disaster in your hands.*
>
> *I have mined your web site & obtained names & address of some/many/most if the folks in san Diego area that got your mailer.*
>
> *Would you like this lack of security & privacy become public knowledge?*
>
> *If you would like to buy my silence, make me an offer I can't refuse.*

10. Additionally, the message contained the names, addresses, and PIN numbers of four San Diego county customers along with a hyperlink to the MNA promotional web site of

http://www.maseratiamerica.com/omaha/default.aspx?upin=ECSD043643. This hyperlink revealed customer information associated with PIN ECSD043643 when clicked. The information provided for all four customers matched what was stored in the MNA database giving credibility to the claim that the web site login was breached and customer data was obtained.

Web Server Log File Analysis

11. The development and maintenance of the MNA Omaha Steaks promotional web site was contracted by MNA to Intelliga Communications. MNA notified Intelliga Communications of the security breach after receiving the email from sol.beach@gmail.com. On March 12, 2008, R. Adam V. Fox, Managing Partner at Intelliga Communications, sent an email to MNA detailing their findings from a review of web server log file activity related to the intrusion. Two Internet Protocol (IP) addresses used for the attacks were identified by Fox.

a. IP address 208.33.48.145 made 93,538 attempts to match PINs on the MNA web site. This activity was done between March 8, 2008, at 6:00 PM EST and ended on March 10, at 7:02 AM EST. IP address location information revealed its location to be in San Diego, California, at Internet Service Provider (ISP) Webside Story.

b. A second IP address of 70.181.210.121 was also used to access the same PIN as accessed by 208.33.48.145 within a three minute time period. IP address location information for this IP address revealed its location to be San Diego, California, at ISP

Cox Communications.

12. On March 18, 2008, I conducted a whois lookup for IP address 208.33.48.145 and 70.181.210.121 to identify their registrants. IP address 208.33.48.145 is registered to Webside Story, 1402 K Street, San Diego, California. Research conducted on the Internet for Webside Story revealed that they were acquired by an Orem, Utah, based company named Omniture, Inc. IP address 70.181.210.121 is registered to Cox Communications, 1400 Lake Hearn Drive, Atlanta, Georgia.

13. On March 24, 2008, R. Adam V. Fox of Intelliga Communications provided me with web server log files for the web site www.maseratiamerica.com and a spreadsheet containing MNA customer database information for San Diego customers. On March 25 and 26, 2008, I conducted a review and analysis of these files. Only two IP addresses were identified as having attempted to login to the website multiple times using different PINs. These were the same IP addresses previously identified by Fox of 208.33.48.145 and 70.181.210.121.

a. IP address 70.181.210.121 accessed the PIN login page on 38 separate occasions. The first access was conducted on March 09, 2008, at 2:46:58 Greenwich Mean Time (GMT) using PIN ECSD019435. This PIN was issued to customer Tammie Thomas of San Marcos, California. Eight additional PINs were unsuccessfully attempted using permutations on the last six digits. Thomas' PIN was accessed once again immediately followed by PIN ECSD019436, a valid PIN issued to customer Bruce Mengler, 682 Villa De La Valle, Solana Beach, California. Following this success, twenty two unsuccessful attempts were made with changes to the last six digits. Four of the five last attempts made from this IP address identified valid PINs.

b. All requests made from IP address 208.33.48.145 have an identical User Agent string of "Wget/1.10.2+(Red+Hat+modified)". A user agent string is transmitted to the web server by a user's web browser to identify the program making the request and its capabilities. This Wget user agent string belongs to the GNU Wget application, a free, open source command line tool for retrieving files from web servers via Hypertext Transfer Protocol (HTTP). Accessing the MNA promotional website with the Wget tool using the appropriate Uniform Resource Location (URL) and PIN combination results in the download of a web page containing information for the associated customer.

c. A total of 93,544 requests were made to the PIN login page from IP address 208.33.48.145. Incremental sequences of PINs were attempted for ECSD010000 through ECSD050000, ECSD060000 through ECSD099999, ECSD110000 through ECSD122131, and ECSD210000 through ECSD211394. Review of customer and PIN information from the spreadsheet of San Diego customers provided by Fox reveals that 2,626 successful logins and downloads of customer information would have resulted from attempting the aforementioned groups of PINs.

d. The first 11 requests made using Wget have differences in time of 15 seconds or greater using PINs ECSD019435, ECSD019335, ECSD019437, ECSD019438, and ECSD019423. On March 09, 2008 at 04:19:55 GMT the PINs become sequential starting at ECSD010000 and the time between requests shortens to between one and two seconds indicating that the Wget program is being run in an automated or scripted way.

e. When examined together, the activity of IP addresses 70.181.210.121 and 208.33.48.145 reveal a coordinated trial and error testing of the PIN security authentication used by the MNA website for customer login. Once this testing was completed and the attack was known to work, a large sample of possible PINs were queried to identify those that were valid.

f. All PINs used during the attempted logins from both IP addresses begin with "ECSD".

Computer Ownership for IP Address 208.33.48.145

14. On March 27, 2008, I telephonically interviewed Andrew Barney, Systems Administrator of Omniture, Inc. Barney advised that the server with IP address 208.33.48.145 is located at their Network Operations Center (NOC) in San Diego, California. This server belongs to a former employee named Bruce Mengler. Mengler worked at Webside Story as a Database Administrator, but was terminated after Omniture acquired Webside Story. This server was allowed to be hosted on the company's network for Mengler as a condition of his employment. The server was left behind by Mengler after he was terminated and Omniture has not requested that he retrieve it. In response to a subpoena, Omniture, Inc. identified Bruce Mengler as having the home address of 682 Via De La Valle, Solana Beach, California, and dates of employment from July 12, 2004 through February 16, 2008.

Subscriber Information for IP Address 70.181.210.121

15. In response to a subpoena, Cox Communications Inc. provided information for the subscriber assigned IP address 70.181.210.121 between March 08, 2008 11:00 PM EST through March 09, 2008, 4:00 PM EST. This subscriber was identified as Bruce Mengler, 682 Villa De La Valle, Solana Beach, California.

Account Information for Sol.beach@gmail.com

16. On March 24, 2008, in response to a subpoena, Google, Inc. provided subscriber and login information for sol.beach@gmail.com. The user provided name for the account was "sol beach" and it was created on August 30, 2004. The following relevant login information was also provided:

a. On March 08, 2008, at 3:33:57 PM GMT, a login occurred from IP address 70.181.210.121. This is the same IP address that participated in the attack and was issued to Bruce Mengler by Cox Communications at this date and time.

b. On March 09, 2008, at 8:38:29 PM GMT, a login occurred from IP address 70.181.210.203. This IP address was issued to Bruce Mengler by Cox Communications at this date and time.

c. On March 11, 2008, at 11:03:20 PM GMT, a login occurred from IP address 72.11.241.3. A whois query at www.arin.net reveals this IP address is registered to MIR3 Inc., 3398 Carmel Mountain Road, San Diego, California. On April 02, 2008, I conducted a check of this location and found that the vehicle registered to Bruce Mengler with California license plate "CPUWZRD" was located in the parking lot. MIR3 Inc. is an information technology company where Bruce Mengler is believed to be currently employed.

COMPUTER SEARCH PROTOCOL

17. With the approval of the court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers that may be found on the premises which may contain information subject to seizure pursuant to this warrant:

Forensic Imaging

a. There is probable cause to believe that any computers encountered during this search contain data that, in addition to being evidence of the enumerated crimes as provided at Rule 41(c)(1), Fed.R.Crim.P., are instrumentalities of the offenses in that there is probable cause to believe that they may contain contraband and fruits of crime as provided at Rule 41(c)(2)and/or were used in committing crime as provided at Rule 41(c)(3). Consequently, the computer equipment, including any external storage devices are subject to seizure and will be seized and transported offsite for imaging. A preliminary analysis of the images will be conducted within thirty (30) days to confirm that the computers either contain contraband or were used in committing the subject offenses. If so, the computers will not be returned. If not, any computer without obvious evidence of containing contraband or of being used in the commission of the enumerated offenses will be returned to its owner. For computers that are retained, the owner may apply in writing to the undersigned for return of specific data not otherwise subject to seizure for which the owner has a specific need. The Federal Bureau of Investigation will reply in writing. In the event that the owner's request is granted, arrangements will be made for a copy of the requested data to be obtained by the owner. If the request is denied, the owner will be directed to Rule 41(g), Federal Rules of Criminal Procedure.

b. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data - data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accessed, unless the access is done by trained professionals using special equipment, methods and software, the operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

c. Special software, methodology and equipment is used to obtain forensic images. Among other things, forensic images normally are "hashed", that is, subjected to a mathematical algorithm to the granularity of 1038 power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

d. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

e. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program which stores data in a non-textual, proprietary manner- ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

f. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

g. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files and take other steps to defeat law enforcement. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

h. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

CONCLUSION

18. Based on the evidence gathered to date, there is probable cause to believe that one or more computer systems at the residence of Bruce Charles Mengler, 682 Via De La Valle, Solana Beach, California 92075 and the computer server owned by Mengler and located at Level 3 as provided herein, were used to illegally access MNA's computer network in violation of Title 18, United States Code, Section 1030(a)(2) and make the extortionate threat to MNA by electronic mail in violation of Title 18, United States Code, Section 875(d) and that evidence of these violations will be found at his residence and in his computers.

//

//

//

//

//

19. Inasmuch as the search warrant will not immediately be executed, and due to the ease with which digital evidence can be destroyed, it is requested that this Court seal the search warrant, application for search warrant and this affidavit.

Travis F. Johnson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 23rd day of April, 2008:

Honorable Jan M. Adler
United States Magistrate Judge